

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-96258

(43) 公開日 平成11年(1999) 4月9日

(51) Int.Cl.⁸ 識別記号

G 0 6 F 19/00

H 0 4 L 9/08

// G 0 9 C 1/00

6 6 0

F I

G 0 6 F 15/24

G 0 9 C 1/00

H 0 4 L 9/00

6 6 0 B

6 0 1 D

審査請求 未請求 請求項の数 5 O L (全 5 頁)

(21) 出願番号 特願平9-256886

(22) 出願日 平成9年(1997) 9月22日

(71) 出願人 000004226

日本電信電話株式会社

東京都新宿区西新宿三丁目19番2号

(72) 発明者 森保 健治

東京都新宿区西新宿三丁目19番2号 日本
電信電話株式会社内

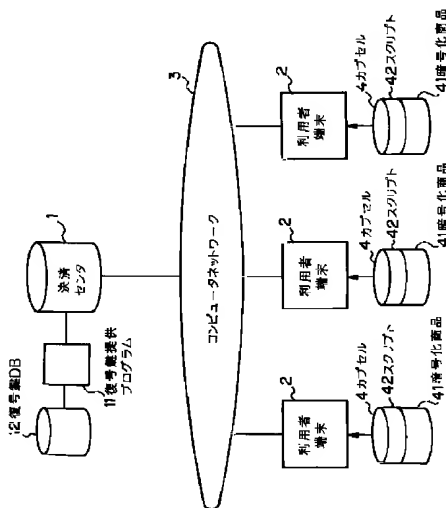
(74) 代理人 弁理士 若林 忠 (外2名)

(54) 【発明の名称】 デジタル情報の利用権販売方法およびシステム

(57) 【要約】

【課題】 暗号化したデジタル情報を商品とする利用権販売システムの多様な料金設定方式に柔軟に対応する。

【解決手段】 商品の復号鍵が登録される復号鍵データベースDB12と復号鍵提供プログラム11を有する決済センタ1と、複数の利用者端末2と、決済センタ1と各利用者端末2とを接続するネットワーク3とからなり、各利用者端末2には暗号化した商品41及びこの商品の複数の利用条件を記述したスクリプト42を含むカプセル4を予め配布し、利用者は、必要ときに、ネットワーク3を介して利用する商品名と決済に必要な情報を決済センタ1に送り、決済センタ1は、この情報と交換にDB12に登録された復号鍵をオンラインで送付し、各利用者は、送付された復号鍵とスクリプト42に記述された利用条件とにより暗号化された商品のデジタル情報を復号して利用する。



【特許請求の範囲】

【請求項1】 デジタル情報を商品として、センタからネットワークを介して複数の利用者端末に販売するデジタル情報の利用権販売方法において、情報提供者が前記商品のデジタル情報を暗号化してその復号鍵をセンタに登録し、前記商品の課金と利用条件に関する情報を含む利用権獲得情報をスクリプトとして記述し、前記スクリプトと暗号化した商品とを一体化してカプセルとして各利用者端末に予め配布し、前記配布されたスクリプトに従って各利用者が入力する復号鍵要求情報を前記センタに送信し、前記各利用者端末から送信された復号鍵要求情報に基づいて復号鍵を当該利用者端末に送信すると共に、当該商品の利用料金の決済を行ない、各利用者端末は送信された復号鍵と前記スクリプトとにより前記暗号化された商品を再生して利用することを特徴とするデジタル情報の利用権販売方法。

【請求項2】 前記スクリプトに記述される情報は、複数の利用条件と各利用条件に対応する課金の情報と、前記複数の利用条件のそれぞれに対応する利用者端末の制御情報とを含み、センタから送信される復号鍵は、デジタル情報の復号鍵情報と当該利用者端末の利用条件を指定する情報とを含む請求項1に記載のデジタル情報の利用権販売方法。

【請求項3】 前記各利用者が利用者端末に入力する情報は、カプセルの商品名及び料金の決済手段に関する情報を含み、各利用者端末は、復号鍵要求情報をセンタに繰返して複数回送信することができる請求項1または2に記載のデジタル情報の利用権販売方法。

【請求項4】 デジタル情報が商品として、センタからネットワークを介して複数の利用者端末に販売されるデジタル情報の利用権販売システムにおいて、前記商品のデジタル情報を暗号化して、その復号鍵をセンタに登録する手段と、前記商品を利用するための利用権獲得情報が記述されるスクリプトと、前記スクリプトと暗号化された商品とを一体化して利用者端末に予め配布されるカプセルと、利用者端末において前記カプセルからスクリプトを読み出して表示する利用権獲得情報表示手段と、前記表示された利用権獲得情報に基づいて入力される復号鍵要求情報の入力手段と、前記復号鍵要求情報を前記センタに転送する要求情報転送手段と、転送された前記復号鍵要求情報の妥当性を確認し、要求された商品の復号鍵を要求元の利用者端末にオンラインで送付する復号鍵送付手段と、前記送付された復号鍵により前記カプセルの暗号化されたデジタル情報を復号して前記商品を再生、表示する

商品再生手段と、

前記商品再生手段の動作状態を計測する利用状態計測手段とを有することを特徴とするデジタル情報の利用権販売システム。

【請求項5】 センタと複数の各利用者端末との間を接続するネットワークとしてインターネット回線が用いられる請求項4に記載のデジタル情報の利用権販売システム。

【発明の詳細な説明】**【0001】**

【発明の属する技術分野】本発明は、ネットワークを介して暗号化されたデジタル情報の商品を販売し、その商品の利用に応じて料金を徴収するデジタル情報の利用権販売方法およびそのシステムに関する。

【0002】

【従来の技術】上述の、商品である情報内容の利用状況に応じて料金を徴収する利用権販売型の方式、以下ペイ・パー・ビュー（PPV）方式という、としては、例えば、視聴した番組の本数に応じて料金を支払うビデオ・オン・デマンド方式のケーブルテレビ、番組を符号化またはスクランブル化等により暗号化して放送し、この放送電波を元の番組に復元するために必要な復号装置を各加入者側に設けて、この復号装置の使用料金を支払う加入者のみが受信可能とする加入テレビジョン方式、あるいは契約条件に基づいて音楽番組をオンラインで提供する通信カラオケ等が知られている。これらのPPV方式では、料金の算定基準が、商品単位、利用時間単位等としてシステムごとに一律に設定されていた。

【0003】商品を暗号化して販売する方式では、デジタル情報を暗号化して適当な手段により予め特定の複数の利用者に配布し、各利用者が必要とときに、ネットワークを経由して暗号化された情報の復号鍵に登録されているセンタに要求してオンラインで復号鍵を入手し、暗号化される前のデジタル情報を再生して利用するシステムがある。この場合、暗号化情報を利用者に配布する手段としては、暗号化したデジタル情報をCD-ROM等の記憶媒体に格納して配布する方法と、ネットワークを経由してダウンロードする方法のいずれかが用いられる。また、PPV方式の場合の暗号化商品の復号鍵は、利用者に提供はされるがその内容は秘匿されていて、センタ以外で複製不可能のように生成される。

【0004】

【発明が解決しようとする課題】上述の従来の利用権販売方式では、1つのシステム内では商品単位、利用時間単位等の1つの料金体系しか設定できない、あるいは個々の商品ごとに異なる料金体系とすることができないという問題点があり、料金体系を変更するためにはシステム全体を改造しなければならなかった。

【0005】しかし、ペイ・パー・ビュー方式においては、商品毎、時間単位等の単独設定のみではなく、利用

回数毎とか部分機能別等、あるいは、これらの組合せの料金設定とか、利用者ごとに異なる組合せの料金体系を必要とすることがある。しかも、一旦設定されたこれらの料金体系も、商品の販売戦略とともにしばしば変更を余儀なくされる。

【0006】また、この利用権販売システムを実現するための設備も、各システムごとに専用の端末や専用の回線が必要になり、近年普及したパーソナルコンピュータやインターネットなどの手軽な基盤技術を利用できないという問題点もあった。すなわち、復号鍵や利用料金決済のための、例えばクレジットカードの暗証番号等の正確性と秘匿性を求められるデータをオンラインで安全に送受信するためには信頼性の高い端末や回線が必要である。

【0007】本発明の目的は、上述の問題点を解消し、商品ごとに料金設定を柔軟に行なうことができるデジタル情報の利用権販売方法およびシステムを提供することにある。

【0008】

【課題を解決するための手段】本発明のデジタル情報の利用権販売方法は、情報提供者が商品のデジタル情報を暗号化してその復号鍵をセンタに登録し、商品の課金と利用条件に関する情報を含む利用権獲得情報をスク립トとして記述し、スク립トと暗号化した商品とを一体化してカプセルとして各利用者端末に予め配布し、配布されたスク립トに従って各利用者が入力する復号鍵要求情報をセンタに送信し、各利用者端末から送信された復号鍵要求情報に基づいて復号鍵を当該利用者端末に送信すると共に、当該商品の利用料金の決済を行ない、各利用者端末は送信された復号鍵と予め配布されたスク립トとにより暗号化された商品を再生して利用することを特徴とする。

【0009】また、スク립トに記述される情報は、複数の利用条件と各利用条件に対応する課金の情報と、複数の利用条件のそれぞれに対応する利用者端末の制御情報とを含み、センタから送信される復号鍵は、デジタル情報の復号鍵情報と当該利用者端末の利用条件を指定する情報とを含むのが望ましい。

【0010】また、各利用者が利用者端末に入力する情報は、カプセルの商品名及び料金の決済手段に関する情報を含むのが望ましい。

【0011】本発明のデジタル情報の利用権販売システムは、商品のデジタル情報を暗号化して、その復号鍵をセンタに登録する手段と、商品を利用するための利用権獲得情報が記述されるスク립トと、スク립トと暗号化された商品とを一体化して利用者端末に配布されるカプセルと、利用者端末においてカプセルからスク립トを読み出して表示する利用権獲得情報表示手段と、表示された利用権獲得情報に基づいて入力される復号鍵要求情報の入力手段と、復号鍵要求情報をセンタに転送

する要求情報転送手段と、転送された復号鍵要求情報の妥当性を確認し、要求された商品の復号鍵を要求元の利用者端末にオンラインで送付する復号鍵送付手段と、送付された復号鍵によりカプセルの暗号化されたデジタル情報を復号して商品を再生、表示する商品再生手段と、商品再生手段の動作状態を計測する利用状態計測手段とを有する。

【0012】また、センタと複数の各利用者端末との間を接続するネットワークとしてインターネット回線を用いてもよい。

【0013】

【発明の実施の形態】次に、本発明の実施の形態について図面を参照して説明する。

【0014】図1は本発明のデジタル情報の利用権販売システムの1実施例のブロック図、図2は図1のシステムのプログラムのモジュール構成図である。

【0015】図1において、本実施例のシステムは、商品の暗号化したデジタル情報の復号鍵が登録されるデータベース12及び復号鍵提供プログラム11を有する決済センタ1と、暗号化された商品41を含むカプセル4が配布され、この暗号化商品の復号鍵を要求して決済センタ1から提供される復号鍵で暗号化商品41を再生して利用するパーソナルコンピュータ等の複数の利用者端末2と、決済センタ1と複数の利用者端末2とを接続するインターネット等のコンピュータネットワーク3とからなる。各利用者端末2に配布されるカプセル4には、暗号化された商品41の他にこの商品の課金と複数の利用条件に関する利用権獲得情報が記述されたスク립ト42が含まれる。

【0016】スク립ト42に記述される利用権獲得情報は、例えば、次のようなものである。

【0017】A) 時間当たり、利用回数当たり、機能別等の課金単位

B) 支払い済みの利用料金と繰り返し利用の可否

C) 支払いのタイミング、(利用前、利用後、利用中) スクリプトの内容は、例えば、料金前払いで、制限時間内には30回までの任意の数の商品の再生が可能という条件の場合の記述は次のようになる。

【0018】[General Info]

CONTENT ID = 1	: 商品 ID
CONTENT ID = 2	: 商品 ID
CONTENT ID = 3	: 商品 ID
CHARGE METHOD = PREPAY	: 前払い

[Time Constraint]

TIME UNIT = HOUR	: 時間単位 (時間)
FEE PER UNIT = 1000	: 単位当たりの金額 (円)
REPLAY = OK	: 同一商品の複数回の再生可

[Count Constraint]

COUNT UNIT = PLAY	: 単位回数 (再生回数)
COUNT LIMIT = 30	: 最大再生回数

【0019】各利用者端末2は、利用者から所望の商品の復号鍵を要求するための商品名及びクレジット暗証番号等の料金決済のための情報のデータが入力されるユーザ入力部21と、ユーザ入力部21に入力されたデータを決済センタ1に送り、当該商品の復号鍵を取得する復号鍵取得部26と、暗号化された商品41を復号するカプセル復号部25と、復号された商品41のデジタル情報を再生、表示する商品再生部24と、商品の利用時間、利用回数、部分機能別等の利用状況を計測する利用状態計測部23と、決済センタ1から送付された復号鍵とカプセル4中のスクリプト42、及び利用状態計測部23の計測結果により、カプセル復号部24と商品再生部24の動作を制御するPPV制御部22と、を含む。

【0020】次に、このシステムの運用について説明する。

【0021】情報提供者は、商品を暗号化してその復号鍵を用意し、決済センタ1の復号鍵データベースDB12に登録する。そして、本システムにおける利用条件を記述したスクリプト42と暗号化された商品41とを合わせて1つのカプセル4として利用者に配布する。この配布には、コンピュータネットワーク3を利用してもよいし、商品が大容量であれば、CD-ROM等の記憶媒体を用いてもよい。

【0022】カプセル4を配布された利用者がその商品を利用しようとするときは、まず、カプセル復号部25が読み出したスクリプト42に応じてGUI (Graphical User Interface) により表示される指示に従ってユーザ入力部21からカプセル4のファイル名と、利用のための決済手段の情報(クレジット番号など)とのデータを入力する。

【0023】PPV制御部22は、例えば、商品の再生、表示の場合は、まず、復号鍵取得部26に指示して、決済センタ1の復号鍵提供プログラム11により復号鍵DB12から復号鍵を獲得する。すなわち、復号鍵取得部26がこのデータをコンピュータネットワーク3を介して決済センタ1に送ると、復号鍵提供プログラム11がこのデータの妥当性をチェックして利用料金の決済処理を行なうと共に、復号鍵DB12から要求された復号鍵を取り出して、この復号鍵をコンピュータネットワーク3を介して要求元の利用者端末2の復号鍵取得部26に送る。

【0024】次に、カプセル復号部25に指示してこの復号鍵により商品41を復号する。復号された商品41は、自動的に商品再生部24に送られて再生、表示される。この際、利用状態計測部23は、利用回数、利用時間等の利用者の商品利用状況を計測して逐次PPV制御部22に通知する。

【0025】PPV制御部22は、利用状態計測部23

からの情報も参照して、商品再生部24による商品41の再生、表示を終了させたり、追加料金が必要とか、次の商品の購入申込みを行なうか等の表示をして利用者にユーザ入力部21からの入力を促す等の制御も行なうことができる。

【0026】例えば、前述のスクリプトの例では、1時間当たり1,000円の商品の例が記載されているが、仮に商品IDの2が3時間の映画であったとすると、この映画を全部見るためには、3回センタに接続して1,000円ずつ支払う必要がある。これを、最初に3,000円支払って1回の接続で済ませる販売形態とすることも可能であり、どちらの販売/利用形態を選択するかは、商品の提供者、乃至は利用者の自由であり、本発明の柔軟性といえることができる。

【0027】また、決済センタと各利用者端末との間の通信には、すでに開発された秘密通信プロトコルや、ネットワークの中間のデータ改竄を防止するチェックデータ付加方式の技術を用いて、決済情報と復号鍵の伝送の信頼性を高めることができる。

【0028】
【発明の効果】上述のように本発明は、スクリプトの設定が柔軟なので、多様なペイ・パー・ビュー方式を一般的なパーソナルコンピュータ上で実現できる効果がある。

【0029】また、予め商品を暗号化して配布しているので、利用時に広帯域ネットワークやISDNのような高速な回線を利用してダウンロードの必要がなく、通常の電話回線でも実現可能であるという効果がある。

【図面の簡単な説明】

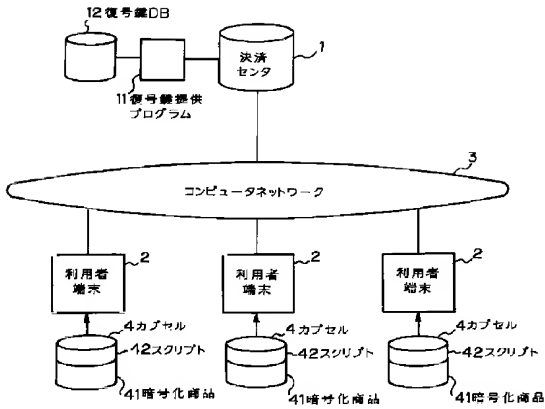
【図1】本発明のデジタル情報の利用権販売システムの1実施例のブロック図である。

【図2】図1のシステムのプログラムのモジュール構成図である。

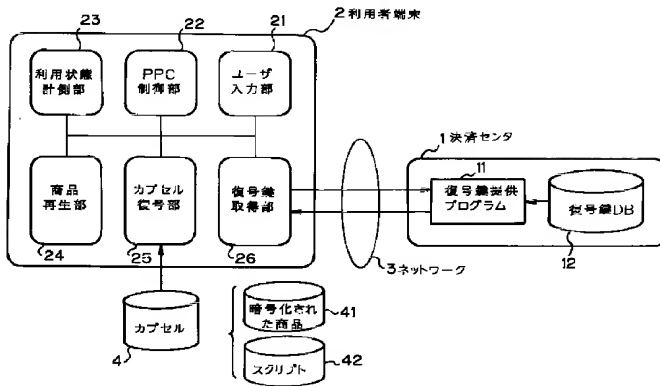
【符号の説明】

- 1 決済センタ
- 2 利用者端末
- 3 ネットワーク
- 4 カプセル
 - 11 復号鍵提供プログラム
 - 12 復号鍵DB
 - 21 ユーザ入力部
 - 22 PPV制御部
 - 23 利用状態計測部
 - 24 商品再生部
 - 25 カプセル復号部
 - 26 復号鍵取得部
 - 41 暗号化された商品
 - 42 スクリプト

【図1】



【図2】



METHOD AND SYSTEM FOR SELLING UTILIZATION RIGHT OF DIGITAL INFORMATION

Publication number: JP11096258 (A)

Publication date: 1999-04-09

Inventor(s): MORIYASU KENJI

Applicant(s): NIPPON TELEGRAPH & TELEPHONE

Classification:

- **international:** G06Q50/00; G06F19/00; G06F21/24; G06Q10/00; G06Q30/00; G09C1/00; H04L9/08; G06Q50/00; G06F19/00; G06F21/00; G06Q10/00; G06Q30/00; G09C1/00; H04L9/08; (IPC1-7): G09C1/00; G06F19/00; H04L9/08

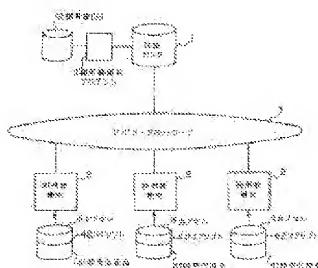
- **European:**

Application number: JP19970256886 19970922

Priority number(s): JP19970256886 19970922

Abstract of JP 11096258 (A)

PROBLEM TO BE SOLVED: To flexibly cope with various charge setting methods of a utilization right sale system to define ciphered digital information as merchandise. **SOLUTION:** The utilization right sale system is constituted of a decoding key database DB12 in which a decoding key of the merchandise is registered, a settlement center 1 provided with a decoding key providing program 11, plural user terminals 2 and a network 3 to connect the settlement center 1 with each user terminal 2, a capsule 4 including ciphered merchandise 41 and a script 42 in which plural utilization conditions of the merchandise are preliminarily described is preliminarily distributed, a name of the merchandise to be utilized and information required for settlement are transmitted to the settlement center 1 with the network 3 when they are necessary by a user.; the decoding key registered in the DB12 is transmitted in on-line in exchange of the information by the settlement center 1 and digital information of the ciphered merchandise is decoded and utilized by the transmitted decoding key and the utilization conditions described in the script 42 by each user.



Data supplied from the **esp@cenet** database — Worldwide